

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2015/2016

TPB3141 – PASSWORD AUTHENTICATION AND BIOMETRICS

(All sections / Groups)

17 OCTOBER 2015

9.00 a.m – 11.00 a.m

(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 9 pages, excluding the cover page, with 10 MCQs and 6 questions only.
2. Attempt **ALL** questions in **Section A**.
3. Attempt **FIVE** out of **SIX** questions in **Section B**. All questions carry equal marks and the distribution of the marks for each question is given.
4. Please print all your answers in the Answer Booklet provided.

SECTION A: Please attempt ALL multiple choice questions. [10 marks]

1. _____ is the process of validating the claimed identity of an end computer, network user or a device such as a host computer, or router.
 - a. Authorization
 - b. Authentication
 - c. Identification
 - d. Validation

2. A _____ is a user setting for biometric systems operating in the verification or open-set identification (watch list) task.
 - a. range
 - b. threshold
 - c. identity
 - d. function

3. _____ includes the process of providing breeder documents, identity history, credentials and documents to establish an identity to an organization that can issue identity credentials.
 - a. Identity registration
 - b. Identity proofing
 - c. Identity verification
 - d. Identity authorization

4. _____ refers to an application of combining data from two or more biometric sensors, such as synchronized reflective-based and temperature-based face images.
 - a. Multimodal
 - b. Multisensory
 - c. Multifactor
 - d. Multifusion

5. _____ is the ability to prove that a specific action occurred in an electronic transaction.
 - a. Repudiation
 - b. Nonrepudiation
 - c. Confidentiality
 - d. Integrity

Continued

6. _____ is surreptitiously obtaining data from an unknowing end user who is performing a legitimate function.
- a. Spoofing
 - b. Skimming
 - c. Eavesdropping
 - d. Mimic
7. Which of the following is NOT a biometrics evaluation criterion?
- a. Acceptability
 - b. Circumvention
 - c. Maintenance
 - d. Performance
8. _____ is a short range wireless communication technology based on RFID technology which is using magnetic field induction. One of the popular applications is Google wallet.
- a. Active RFID
 - b. Optical communication
 - c. Near field communication (NFC)
 - d. Synchronization protocol
9. _____ utilizes the distinctive aspects of the subcutaneous patterns (beneath the skin) in an individual's hand.
- a. Palmprint recognition
 - b. Fingerprint recognition
 - c. Vein recognition
 - d. Hand geometry recognition
10. _____ is a common situation in which users have multiple identities and passwords across a variety of networks, web sites, applications, computers or computing devices.
- a. Password synchronization
 - b. Password composition rule
 - c. Password chaos
 - d. Transitive thrust

Continued

SECTION B: Please attempt FIVE out of SIX questions only**Question 1:**

- a) Fill in the blanks with the most appropriate authentication service:
- i. _____: A computer network authentication protocol which works on the basis of “tickets” to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
 - ii. _____: An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
 - iii. _____: Users can access multiple systems after providing credentials only once.
 - iv. _____: An Extensible Markup Language (XML)-based data format used for single sign on (SSO) on Web browsers.
 - v. _____: A protocol developed by Cisco that handles authentication, authorization, and accounting (AAA) services.

[5 marks]

- b) Three of the central concepts in the information security are identification, authentication, and authorization. With your security knowledge, distinguish their concepts by providing an example for each of them.

[3 marks]

- c) Today's competitive business environment demands options that offer more protection when network resources include highly sensitive data, thus, using a password-based authentication may not sufficient. Suggest **FOUR** [4] possible ways where a password can be easily compromised.

[2 marks]

Continued

Question 2:

- a) Intruder lockout mechanism is effective to prevent a series of password guessing attacks against a single account. However, this mechanism can be also used by hackers to carry out a denial-of-service (DoS) by intentionally locking out victims' accounts. Considering this limitation, suggest **THREE** [3] appropriate ways of enforcing intruder lockout mechanism.

[3 marks]

- b) The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. With your best knowledge, evaluate the effectiveness of MD5, SHA-2 and HMAC.

[3 marks]

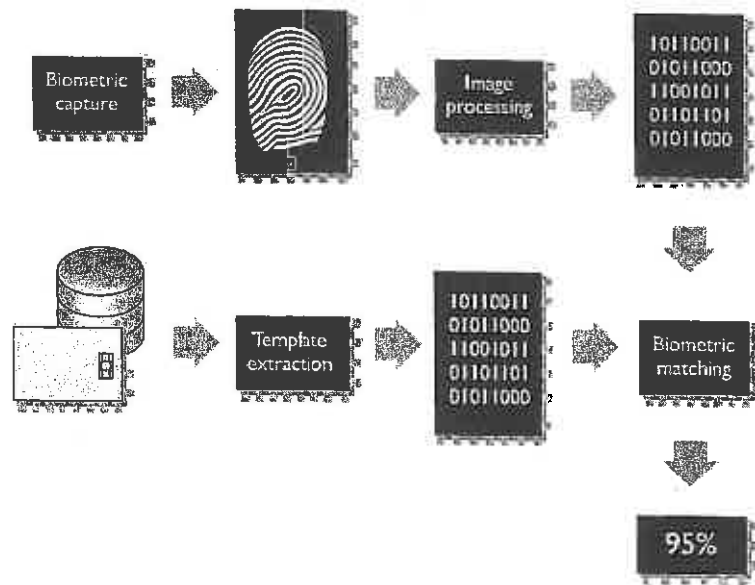
- c) Barcodes have become a universal tool used by organizations to identify the goods in supply chain management since the early 1970s. However, its usage is very labor-intensive as the barcodes have to scan individually and lack of traceability. Considering these limitations, propose another token-based automatic identification system to improve the efficiency and reliability of the entire chain by ensuring that the right goods are available in the right place with no discrepancies and zero errors. Evaluate your proposal by illustrating how it works.

[4 marks]

Continued

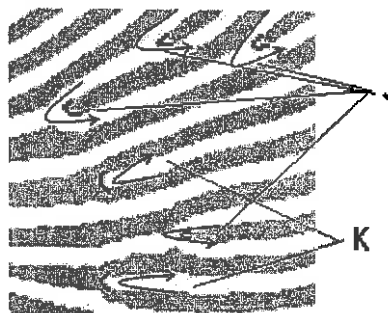
Question 3:

- a) Refer to the figure below, “the verification rate of this biometric system is 95%, thus the Equal Error Rate (EER) is equal to 5%”. Do you agree with this statement? Justify your answer.



[3 marks]

- b) Minutiae are termed as points of ‘significant turn’ on the contour, including ‘left turn’ which is known as J; and ‘right turn’ which is known as K. Name J and K, respectively.



[2 marks]

Continued

- c) The international trading company – Richest Company has many branches all over the world and massive trading information are sent across the network every day. Considering the administrator-level accounts may have a wide range of user rights, compromising these accounts can lead to disastrous consequent to the company business. As a security administrator of the company, you are required to ensure the reliable authentication to the network resources by considering the following requirements given by the company CEO:

- Reliable identification – High
- Response time – High
- Scalability – High
- Deployment cost – Low to medium

There are three options available: (i) passwords, (ii) smart card with PIN, and (iii) biometrics. Make the decision and evaluate your choice.

[5 marks]

Continued

Question 4:

- a) Identify the numbers of core point, delta point and categorize the following four images based on the fingerprint classes.



Image 1



Image 2



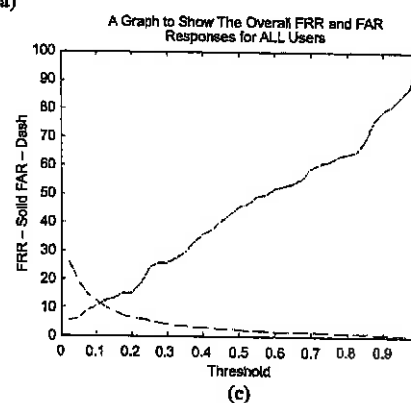
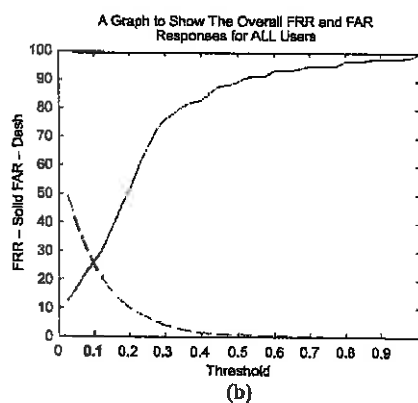
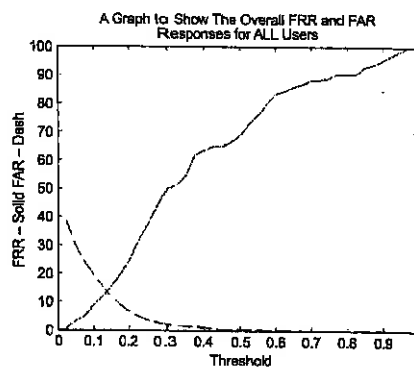
Image 3



Image 4

[6 marks]

- b) You are developing a hand geometry attendance system for Multimedia University. Three research techniques *a*, *b*, and *c* are tested and their performances are illustrated in the graph below. Which technique you will choose? Justify your answer.



[4 marks]

Continued

Question 5:

- a) You are leading a research project on face recognition system. To evaluate your own feature extraction algorithm, you are considering two classical benchmark techniques, which are principal component analysis (PCA) and linear discriminant analysis (LDA). With your best knowledge, distinguish both of them. An illustration can be used to support your justification.

[4 marks]

- b) Without considering the current computing capabilities, do you think palmprint recognition system is better than fingerprint recognition system? Justify your answer.

[4 marks]

- c) Define BioAPI and discuss the importance of its implementation.

[2 marks]

Continued

Question 6:

- a) Amazon has patented a system by using individuals' unique ear shapes as smartphone-unlocking passwords. The technology is used to unlock a phone when a person gets a call, with the technology automatically recognizing the person's ear shape. This would enable users to get into that phone without a password or specific PIN.

Evaluate the feasibility of ear biometrics by providing **FOUR [4]** advantages of it as of compared to the face biometrics.

[4 marks]

- b) The number of courses being offered online is growing by the day. However, it is very hard and almost impossible to monitor the students' online learning activities.

Propose **ONE [1]** behavioral biometric authentication solution to prevent the academic dishonesty and fraud. Justify your answer.

[2 marks]

- a) Facebook rolled out a new service called "Moments" that expands the use of the company's powerful faceprint technology in June 2015. "Moments" automatically scans the users' camera roll on their smartphone for photos of their friends by using Facebook's sophisticated facial recognition software. It then lets the users to send over the photos to the friends identified in them.

Discuss this issue by relating the "Moments" deployment to the privacy continuum.

[4 marks]

End of Page